

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**UTILITY PATENT APPLICATION TRANSMITTAL**  
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 74451.P100

Total Pages 3

First Named Inventor or Application Identifier Jonathan J. Hull

Express Mail Label No. EL234218784US

**ADDRESS TO:** Assistant Commissioner for Patents  
Box Patent Application  
Washington, D. C. 20231

**APPLICATION ELEMENTS**

See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form  
(Submit an original, and a duplicate for fee processing)
2. X Specification (Total Pages 24)  
(preferred arrangement set forth below)
  - Descriptive Title of the Invention
  - Cross References to Related Applications
  - Statement Regarding Fed sponsored R & D
  - Reference to Microfiche Appendix
  - Background of the Invention
  - Brief Summary of the Invention
  - Brief Description of the Drawings (if filed)
  - Detailed Description
  - Claims
  - Abstract of the Disclosure
3. X Drawings(s) (35 USC 113) (Total Sheets 4)
4. X Oath or Declaration (Total Pages 5)
  - a.      Newly Executed (Original or Copy)
  - b.      Copy from a Prior Application (37 CFR 1.63(d))  
(for Continuation/Divisional with Box 17 completed) (**Note Box 5 below**)
  - i.      DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5.      Incorporation By Reference (useable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6.      Microfiche Computer Program (Appendix)

7. ☐ Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, all necessary)  
a. ☐ Computer Readable Copy  
b. ☐ Paper Copy (identical to computer copy)  
c. ☐ Statement verifying identity of above copies

**ACCOMPANYING APPLICATION PARTS**

8. ☐ Assignment Papers (cover sheet & documents(s))  
9. ☐ a. 37 CFR 3.73(b) Statement (where there is an assignee)  
☐ b. Power of Attorney  
10. ☐ English Translation Document (if applicable)  
11. ☐ a. Information Disclosure Statement (IDS)/PTO-1449  
☐ b. Copies of IDS Citations  
12. ☐ Preliminary Amendment  
13. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)  
14. ☐ a. Small Entity Statement(s)  
☐ b. Statement filed in prior application, Status still proper and desired  
15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)  
16. ☐ Other: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

17. **If a CONTINUING APPLICATION**, check appropriate box and supply the requisite information:  
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP)  
of prior application No: \_\_\_\_\_

**18. Correspondence Address**

☐ Customer Number or Bar Code Label \_\_\_\_\_  
(Insert Customer No. or Attach Bar Code Label here)  
or

☒ Correspondence Address Below

NAME Michael J. Mallie Reg. No. 36,591  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard  
Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

12/01/97

- 2 -

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032  
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR PUBLISHING DOCUMENTS OVER A  
NETWORK

Inventors:

Jonathan J. Hull  
Marko Balabanovic  
Peter Hart  
Greg Wolff

Prepared by:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP  
12400 Wilshire Boulevard, Seventh Floor  
Los Angeles, California 90025  
(310) 207-3800

**EXPRESS MAIL CERTIFICATE OF MAILING**

"Express Mail" mailing label number: EL234218784US

Date of Deposit: September 17, 1999

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D. C. 20231

Sharon M. Osofsky

(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

(Date signed)

September 17, 1999

# METHOD AND APPARATUS FOR PUBLISHING DOCUMENTS OVER A NETWORK

## BACKGROUND OF THE INVENTION

### Field of the Invention

5           The invention relates to publishing electronic documents over a network, such as a wide area network, the World Wide Web, etc.; more specifically, the invention relates to controlling access to documents accessible over a network.

### Description of Related Art

10           Publishing electronic documents on a network such as a wide area network is known in the art. For example, see U.S. Patent No. 5,870,552 issued to Dozier. These systems are usually client-server systems in which clients make requests to the server, and the server generates responses. Client-server platforms are used for authoring of documents, content-based indexing of documents, retrieval of documents, management and control of documents, and support for developing  
15           form-driven interactive services.

          In typical client-server document systems, a document is stored on a server from which a user accesses, edits, and/or restores the document. While providing users with an opportunity to perform various tasks on a document stored on a server, such systems and the access to documents thereon lack important security  
20           measures. For example, a document stored on a server without some security mechanism (e.g., a security key) does not prevent unscrupulous users from

accessing the document. Moreover, because documents may reside on a server for an indefinite period of time, there is an increased risk that an unauthorized user may gain access to a document. Currently, there is no system that ensures that only authorized users gain access to a document published on a network and that

5 prevents documents from being maintained for long periods of time on a server. It is, therefore, desirable to have a system that uses security measures to prevent unauthorized individuals from gaining access to documents residing on a server and that reduces the risk of unauthorized access.

## SUMMARY OF THE INVENTION

A system for publishing an electronic document on a network is described.

In one embodiment, the system comprises a document source, a filter, and a server.

The document source supplies an electronic document. The document source may

5 be a multifunction machine. The filter transforms the electronic document for publication. The server has a memory for storing the electronic document and permits access to the electronic document using a document identifier. The server also sends, to a publisher designated location, information regarding accesses to the electronic document.

## BRIEF DESCRIPTION OF THE DRAWINGS

The features, aspects, and advantages of the invention will become more thoroughly apparent from the following detailed description, appended claims, and accompanying drawings in which:

5           **Figure 1** is a block diagram of one embodiment of a document publishing system;

**Figure 2** is a block diagram of one embodiment of a high-level architecture for a typical client-server network;

**Figure 3** shows one embodiment of a computer program with various  
10       modules that may be executed by one or more processing devices; and

**Figure 4** is a flow chart of one embodiment of a process for providing access to an electronic document.

## DETAILED DESCRIPTION OF THE INVENTION

In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it will be understood by one of ordinary skill in the art that the invention may be practiced without these specific  
5 details. In other instances, well known structures and techniques have not been shown in detail in order not to obscure the invention.

Some portions of the detailed descriptions which follow are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the  
10 means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or  
15 magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to  
20 be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent



from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the

description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

## 5 Overview

A publishing system is described that has a source of documents, a filter to filter the documents so that only selected documents are published, and a web server to allow access to selected documents. In one embodiment, the filter transforms the appearance of the document and notifies others that publication has  
10 taken place, e.g., by email. In one embodiment, the filter comprises a computer that stores and sends an electronic document to a server to "publish" the documents. The document is accessed using a document identifier (e.g., a URL). A user name and a password or other security key may also be generated to access the electronic document. The URL and any user name and password are sent to an authorized  
15 user (viewer), thereby enabling the authorized user to access the document. The user name and password or security key may be encoded in the URL itself. Users can optionally publicize a document by emailing the URL to a World Wide Web indexing service (e.g., Yahoo, Altavista, Excite, or an existing publicity service).

In one embodiment, the server receiving the document automatically deletes  
20 it once a predetermined condition has been met. The condition may relate to the number of times a document has been accessed, (e.g., after the document has been

accessed once, a certain number of accesses), amount of time (e.g., 10 days) from the date of first access or publication, or after the document has been successfully downloaded by a user from a specified internet address (IP address), etc. The condition may be established by the publisher of the document or a user.

5           **Figure 1** is a block diagram of one embodiment of a publishing system. The publishing system may comprise a multimedia World Wide Web publishing system where the documents being published are multimedia documents. For example, these documents may include scanned images, sound and/or video clips.

Referring to Figure 1, document source 5 generates documents. In one  
10           embodiment, document source 5 may be capable of performing multiple functions such as, for example, copying, faxing, e-mailing, printing, or scanning an electronic document. The documents may be generated and published as part of performing that function(s). For example, if document source 5 comprises a copier, the  
15           document that is generated for potential publication is the result of performing the copying operation. Saving a copy of a document as a side effect of another process (e.g., copying, printing, faxing, etc.) in the absence of an explicit command by a user to do so is referred to herein as “unconscious” capture.

In one embodiment, document source 5 comprises a multifunction machine, workstation, or scanner. Document source 5 may have a specifically designed  
20           touchscreen interface that controls the publication process. Options available on the interface may include (1) specifying destination web server; (2) specifying level of

security; (3) specifying publicity; (4) specifying email destinations for published URL (document identifier) and password; (5) specifying local output of a document, including printing, faxing, and emailing. Document source 5 may also include facilities for composition of multimedia documents such as audio and video capture devices.

Document source 5 may comprise a printer driver. In such a case, users print to a "webpublish" printer. The document, however, is actually not printed, i.e., paper would not actually be generated, but the postscript or other printer language for the document would be transferred to filter computer 10. Similarly, in one embodiment, users email the document as an attachment to the "webpublish" address.

The generated electronic documents are sent to and received by a filter computer 10. Filter computer 10 comprises a document transformation filter 10A to transform documents into a format suitable for publication. For example, in one embodiment, filter computer 10 may convert Postscript documents into HTML. That is, in one embodiment, software executing on filter computer 10 transforms the documents from document source 5.

In one embodiment, document transformation filter 10A ensures that the document meets certain standards established by a publisher such as the electronic document is free of pornographic or violent material. Additionally, filter computer 10 may prevent documents designated as "confidential" from being published

unless conditions specified by the publisher are met. Filter computer 10 may also filter other information that a publisher wishes to prevent from being published outside of a firewall. Thus, filter computer 10 filters a document of elements that a publisher specifically requests not to be placed on server 15, such as, for example, material deemed to be pornographic, violent, or information designated as proprietary by the publisher. Alternatively, a document may be filtered at a work station used to compose the electronic document. Also filter computer 10 may screen for and remove viruses, especially so called "macro" viruses from, for example, Microsoft Word or PowerPoint documents. Techniques for virus removal are well-known in the art.

Filter computer 10 may also have a database 10B for storing and organizing multiple documents. In one embodiment, filter computer 10 is capable of hosting multimedia data used in composing the document. Filter computer 10 may be embedded either in a multi-functional machine or a single function device, such as, for example, a copier, a facsimile, a printer, a scanner, a smaller device, etc.

Filter computer 10 sends the document(s) to server 15, which may be outside a firewall, for publication. In one embodiment, the connection between filter computer 10 and server 15 may be implemented with an Internet network connection. In another embodiment, this connection may be by a dialup bulletin board server.

After the electronic document is stored on server 15, a user using an interface on a client (not shown) is able to gain access to the electronic document. In one embodiment, the user accesses the document with a document identifier (e.g., a URL). In an alternate embodiment, the URL and an associated user name and password, or security key, are required to access the document. After the user inputs the URL and any necessary user name and password, the user is able to access the electronic document. A user may be notified of the document identifier and/or the password using an e-mail system. Server 15 may also enforce different levels of security.

In one embodiment, filter computer 10 returns the URL for the published document to the original publisher, perhaps by email. Optionally, users of the document source 5 could indicate a password for the document on the print command line.

Server 15 may be located on a private network. In an alternate embodiment, server 15 may be a dialup bulletin board server. Server 15 may be structured as a collection of individual documents or it could be set up as a searchable database of documents. In the latter case, users may be provided with their own home pages that are portals to each user's "collection of documents." A publisher will have access to a list of allowable users at the time at which a document is to be published.

A software system manager for server 15 may be included. The software system manager may run in the background as a Windows Service or Unix daemon.

The system manager monitors the access logs and updates a database of information about who or what systems access which documents at what times. This information would be made available to publishers so they could monitor when their documents are accessed. Thus, server 15 records the number of times a document is accessed, the time of each document access, and/or who obtained access to a document. Server 15 may also notify a publisher that the document has been accessed and specify who accessed it.

Other common system management functions that may be performed by the system manager would include deleting documents. After the electronic document has been accessed by a user a predetermined number of times (e.g., 1, 2, etc.), the system manager server 15 may automatically delete the document depending upon the instructions provided by the publisher or by a user (depending on the implementation) to server 15. The deletion of the document may be based on a specified condition (e.g., the document is deleted after a certain period of time, after all of the authorized users have accessed the document, etc.). For example, at the time documents are published, users would have the option of setting a deletion date. When that date arrives, the system manager would automatically delete the indicated document. This would support the transient use of published documents.

When a document is published, such as when the document is sent to a user's collection of documents, notification may be automatically sent to that user indicating that a document has been sent to his collection of documents. Automatic

notification may be based upon an event designated by the publisher (or user), such as a time period, a condition precedent, a condition concurrent or a condition subsequent. The notification may occur through e-mail by an e-mail based document manager which is part of server 15. The e-mail based manager may have sorting, sending, and receiving capabilities.

In order to receive e-mail notification, users may need a computer executing a program that allows for monitoring and detecting of incoming e-mail. In one embodiment, the software program executing on the user's computer detects receipt of a message notifying the user that he has received e-mail. In one embodiment, the user's computer may execute software that performs an automatic updating process that copies the published document to the user's computer. Such software may be triggered by receipt of the notification message. In one embodiment, the software executing on the computer also sends a command back to web server 15 to remove the published document.

Server 15 may also include an email-based document manager to allow publishers to send an email message to server 15 to obtain a listing of published documents, to add or delete passwords or to delete the document.

**Figure 2** shows client 100 and server 200 with a firewall (optional) between client 100 and server 200. Client 100 has a central processing unit 110, a user input-output device or interface 120, at least one storage unit 130, an operating system 140, and client software 150.



Server 200 contains a central processing unit ("CPU") 210, a user input-output 220, a storage unit 230, an operating system 235, and computer programs for execution thereon. In one embodiment, storage 230 maintains documents and access logs. Access logs record information such as the time a document is accessed, the  
5 number of times a documents has been accessed, and by whom.

The server may include a library of software modules that allow for progressive display of large document images as well as a collection of plug-ins that can be used to display the multimedia data in published documents. **Figure 3** illustrates modules that may be used in a computer program for the server 15 for  
10 easy access and use of the documents stored thereon. Compression/decompression module 300 is used for compressing or decompressing a large quantity of document data or multiple documents stored on server 15. Additionally, progressive transmission and display module 310 may be used for displaying a reduced resolution version of a document image while the system loads a higher resolution  
15 version of the image (*e.g.*, one page of the document is shown at one time and then the next page is transmitted). Encryption/decryption module 320 adds additional security measures to documents, such as, for example, encrypting or decrypting a document, including public key services. Browser module 330 generates and operates a browser, including a customized browser 330 that may be placed on the  
20 server for access by the user.

Moreover, a customized display utilities module 340 allows a user to customize the type of display for certain types of documents on the server. For example, some users may require very complex display utilities based on the type of services required by the user. The user may, for example, be a graphic artist who  
5 needs significant color, sound, and sight capabilities in order to construct a complex media document. This module allows that user to set the type of display parameters that he requires. Modules could be customized by the publisher 350 to allow a publisher to provide customized utilities for his users or for the publisher himself. This may include such items as performing complex mathematical calculations in a  
10 document. System manager module 360 has modules for performing various functions such as maintaining the access logs in which information is recorded such as how many times a document has been accessed, when a document was accessed, and who accessed the document. Additionally, the server manager module 360 may notify a publisher that a document has been accessed or it may notify the user that  
15 an e-mail has been sent and its location on that server.

**Figure 4** is a flow chart of the operation of the publishing system. Referring to Figure 4, the process begins by generating an electronic document, including transforming a document into an electronic format (e.g., HTML) if necessary (processing block 401). The document is then stored on a server (processing block  
20 402). After storing the document (or at the same time), a URL and a password are generated to enable access to the document (processing block 403). The URL can be generated at the source automatically by, e.g., maintaining a counter that is

incremented for each document published at that source. Such a URL might look like <http://www.ricoh.com/45.html> for the 45th published document. The URL could also be generated manually at the source by allowing the user to enter a name for the document. In addition to the automatic URL generation method discussed  
5 above, URLs can be generated automatically on the server by generating a long random number. This has the advantage of providing some level of security. It will be difficult for anyone trying to break into the system to guess such a randomly generated URL.

The password can be generated by the user or publisher at the source. It can  
10 also be generated automatically by the source or filter computer. Such generation may be random generation.

In an alternative embodiment, the resource locator (e.g., URL) and password may be generated prior to storing the document on the server.

The URL and password are then forwarded to one or more users (processing  
15 block 404). In one embodiment, these are forwarded via email. These may be forwarded separately and may be forwarded using offset communication mechanisms.

The URL and (optionally) the password can be emailed by the publisher user to intended recipients. If done from the console of a multifunction machine, the user  
20 interface would include functionality for entering the email addresses or fax phone number of intended recipients. The email or faxing could be performed by the filter

computer or the server. In an alternate embodiment, after the document is stored on the server, the URL and password are returned to the source (e.g., multifunction machine). It then performs the email or faxing of the URL. This has the advantage of supporting remote publishing with locally controlled publicity. The server might  
5 be a public system in which the publisher user does not want to share his list of recipients. It might be a confidential customer list, for example.

Once the URL and password have been obtained, the user accesses the document (processing block 405). The server tests whether a condition has been met (e.g., all authorized users have accessed the document, etc.) (processing block 406).

10 If so, then the server deletes the document (processing block 407) and the processor ends.

In the preceding detailed description, the invention is described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the  
15 broader spirit and scope of the invention as set forth in the claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

## CLAIMS

What is claimed is:

1           1.     A system for publishing an electronic document on a network  
2 comprising:  
3           a multifunction machine to supply the electronic document;  
4           a filter to transform the electronic document for publication;  
5           a server having memory for storing the electronic document, the server  
6 permitting access to the electronic document using a document identifier and  
7 sending, to a publisher designated location, information regarding the number of  
8 accesses that have occurred.

1           2.     The system defined in Claim 1 wherein the number of accesses that  
2 occurred comprises zero or more accesses.

1           3.     The system defined in Claim 1 wherein the multifunction machine  
2 comprises a print driver that publishes the electronic document on a network.

1           4.     The system defined in Claim 1 wherein the document identifier  
2 comprises a URL.

1           5.     The system defined in Claim 1 wherein the server deletes the  
2 document based upon existence of a condition.

1           6.     The system defined in Claim 5 wherein the condition is an access by an  
2 authorized user.

1           7.     The system defined in Claim 5 wherein the condition is a  
2 predetermined time after the document has been stored on the server.

1           8.     The system defined in Claim 1 wherein the server maintains access  
2 logs and updates the access logs each time a document is accessed.

1           9.     The system defined in Claim 1 wherein the server comprises a system  
2 manager.

1           10.    The system defined in Claim 9 wherein the system manager is capable  
2 of accessing access logs.

1           11.    The system defined in Claim 9 wherein the system manager notifies  
2 the publisher that a document was accessed by a user.

1           12.    The system defined in Claim 11 wherein the server manager  
2 automatically sends an electronic mail message to the publisher indicating that the  
3 document was accessed by a user.

1           13.    The system defined in Claim 1 wherein the filter performs virus  
2 removal.

14. A method of publishing an electronic document to a user comprising:  
a multifunction machine unconsciously sending an electronic document to a  
server as part of performing another user specified function;  
sending a network document identifier and password for accessing the  
electronic document;  
accessing the electronic document using the network documents identifier  
and password;  
sending an electronic mail message indicating the number of accesses to the  
electronic document that have occurred.

15. The method defined in Claim 14 wherein sending the electronic  
document comprises a multi-function machine printing the electronic document.

16. The method defined in Claim 14 further comprising generating a  
security key.

17. A computer-implemented method comprising:  
receiving an unconsciously captured electronic document at a server;  
the server allowing access to the electronic document by using a security key  
and a document resource identifier; and  
the server automatically notifying a publisher that an electronic document  
has been accessed.

1 18. The method defined in Claim 17 wherein the server notifies a user that  
2 an electronic mail message containing a URL has been sent from a server.

1 19. The method defined in Claim 17 further comprising preventing access  
2 to the electronic document once a condition exists.

1 20. The method defined in Claim 19 wherein the condition is a  
2 predetermined amount of time has passed.

1 21. The method defined in Claim 19 wherein the condition is the electronic  
2 document has been accessed a predetermined number of times.

1 22. An apparatus comprising:  
2 means for receiving an unconsciously captured electronic document at a  
3 server;  
4 means for allowing access to the electronic document by using a security key  
5 and a document resource identifier; and  
6 means for automatically notifying a publisher that an electronic document  
7 has been accessed.

1 23. The apparatus defined in Claim 22 wherein means for notifying  
2 notifies a user that an electronic-mail message containing a URL has been sent from  
3 a server.



1           24.    The method defined in Claim 22 further comprising means for  
2 preventing access to the electronic document once a condition exists.

1           25.    The method defined in Claim 24 wherein the condition is a  
2 predetermined amount of time has passed.

1           26.    The method defined in Claim 24 wherein the condition is the electronic  
2 document has been accessed a predetermined number of times.

1           27.    The apparatus defined in Claim 22 further comprising means for  
2 generating the security key.

1           28.    An article of manufacture having one or more recordable media  
2 having a plurality of executable instructions stored thereon which, when executed  
3 by a processing device, cause the processing device to:

4           receive an unconsciously captured electronic document at a server;

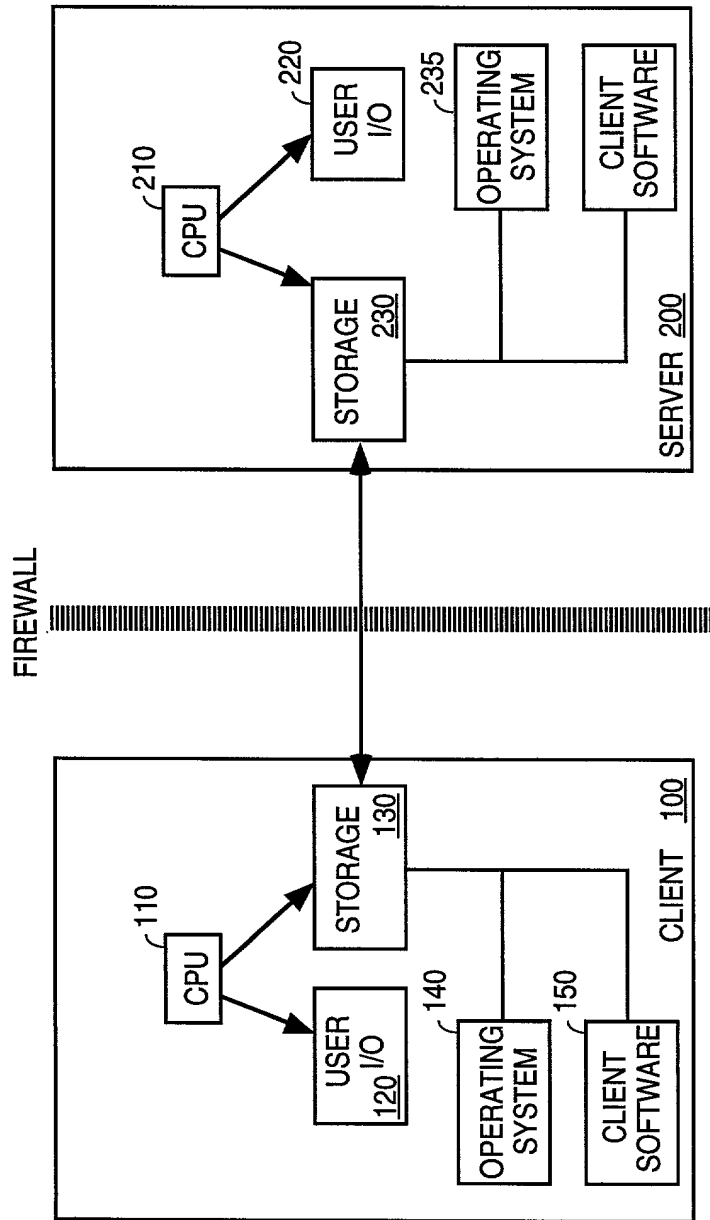
5           allow access to the electronic document by using a security key and a  
6 document resource identifier; and

7           automatically notify a publisher that an electronic document has been  
8 accessed.

## ABSTRACT

An apparatus and method for publishing an electronic document on a network is described. In one embodiment, an apparatus for publishing an electronic document on a wide area network comprising at least one server and a client, a  
5 client having memory for storing an electronic document, and means for sending the electronic document to the server, wherein a URL is associated with the electronic document, a security key associated with the URL, and means for sending a URL to a user.





**Fig. 2**

SERVER COMPUTER PROGRAM  
MODULES

COMPRESSION/DECOMPRESSION  
UTILITIES 300

PROGRESSIVE TRANSMISSION  
310

ENCRYPTION/DECRYPTION  
INCLUDING PUBLIC KEY SERVICES 320

BROWSER INCLUDING  
CUSTOMIZED BROWSER 330

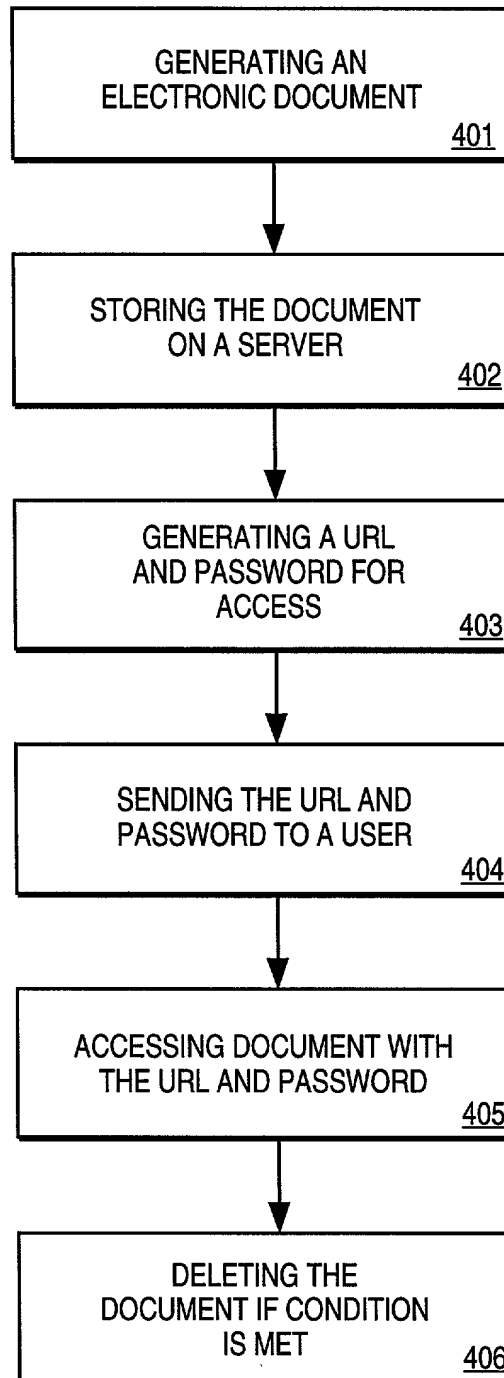
DISPLAY UTILITIES  
INCLUDING CUSTOMIZED  
DISPLAY UTILITIES 340

MODULE FOR RECORDING  
INFORMATION (E.G. WHO ACCESSED  
THE DOCUMENT, HOW MANY TIMES  
THE DOCUMENT HAS BEEN  
ACCESSED) 345

MODULES CUSTOMIZED  
BY THE PUBLISHER 350

THE SERVER HAS A SYSTEM MANAGER  
CAPABLE OF PERFORMING FUNCTIONS  
SUCH AS ACCESSING ACCESS LOGS,  
OR NOTIFYING A PUBLISHER THAT A  
DOCUMENT HAS BEEN ACCESSED 360

**Fig. 3**



**Fig. 4**

As a below named inventor, I hereby declare that:

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

X is attached hereto.  
\_\_\_\_\_ was filed on \_\_\_\_\_ as  
United States Application Number \_\_\_\_\_  
or PCT International Application Number \_\_\_\_\_  
and was amended on \_\_\_\_\_  
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority  
Claimed

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

|                      |             |   |
|----------------------|-------------|---|
| (Application Number) | Filing Date | (Status -- patented,<br>pending, abandoned) |
| (Application Number) | Filing Date | (Status -- patented,<br>pending, abandoned) |

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to Michael J. Mallie, BLAKELY, SOKOLOFF, TAYLOR &  
(Name of Attorney or Agent)

**ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to Michael J. Mallie, (408) 720-8598.**  
**(Name of Attorney or Agent)**

**I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.**



Full Name of Sole/First Inventor Jonathan J. Hull

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Second/Joint Inventor Marko Balabanovic

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Third/Joint Inventor Peter Hart

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

Full Name of Fourth/Joint Inventor Greg Wolff

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence \_\_\_\_\_ Citizenship \_\_\_\_\_  
(City, State) (Country)

Post Office Address \_\_\_\_\_  
\_\_\_\_\_

## APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. P44,587; Yong S. Choi, Reg. No. P43,324; Thomas M. Coester, Reg. No. 39,637; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; Dinu Gruia, Reg. No. P42,996; Willmore F. Holbrow III, Reg. No. P41,845; George W. Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. P44,976; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Kimberley G. Nobles, Reg. No. 38,255; Daniel E. Ovanezian, Reg. No. 41,236; Babak Redjaian, Reg. No. 42,096; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Anand Sethuraman, Reg. No. P43,351; Charles E. Shemwell, Reg. No. 40,171; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Stephen Warhola, Reg. No. 43,237; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. P45,241; Steven D. Yates, Reg. No. 42,242; Ben J. Yorks, Reg. No. 33,609; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and James A. Henry, Reg. No. 41,064; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney.

## APPENDIX B

### Title 37, Code of Federal Regulations, Section 1.56 Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
  - (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.
- (b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and
- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
  - (2) It refutes, or is inconsistent with, a position the applicant takes in:
    - (i) Opposing an argument of unpatentability relied on by the Office, or
    - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
  - (2) Each attorney or agent who prepares or prosecutes the application; and
  - (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.
- (d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.